AO 91 (Rev. 11/11) Criminal Complaint (approved by AUSA Lesley Bonney)

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.
THEODORE PRICE

Case No. 17-945-M

Defendant(s)

AMENDED CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 1/1/17 and 7/12/17 in the county of Montgomery in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 1028(a)(7)	Identity theft
18 U.S.C. 1029(a)(3)	Access device fraud

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

SA Emily J. Evans, Homeland Security Investigations

Printed name and title

Sworn to before me and signed in my presence.

Date: July 18, 2017

Judge's signature

City and state: Philadelphia, PA

Hon. Timothy R. Rice, USMJ

Printed name and title

AFFIDAVIT

I, Emily J. Evans, being duly sworn, state as follows:

1. I am a Special Agent with Homeland Security Investigations ("HSI"), and have been so employed since March 2007. Since becoming a Special Agent, I have participated in numerous investigations into suspected computer related crimes. I am currently assigned to the Philadelphia Special Agent in Charge HSI Office, Cyber Crimes Group. I hold a Bachelor of Science in Business Administration from The Ohio State University, with a focus in Marketing and Transportation/Logistics.

2. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered to conduct investigations of, and to make arrests for, the offenses enumerated in Titles 8, 18, 19, 21, and 31 of the United States Code and other related offenses.

3. I am responsible for investigations focusing on the use of computers to commit crimes including, but not limited to, identity theft, access device fraud, and other computer crimes. As a law enforcement officer, I have participated in numerous searches and arrests, debriefings of criminal defendants and confidential sources, initiation and monitoring of pen registers and trap and trace devices, and monitoring of authorized wire communication intercepts. As such, I am familiar with the use of computers to commit crimes such as identity theft and access device fraud.

4. The information contained in this affidavit is based on my personal observations, my training and information provided by other law enforcement officers and/or agents. This affidavit sets forth only those material facts that I believe are necessary to establish probable

cause for a criminal complaint. It does not include each and every fact of this investigation.

5. I submit this affidavit in support of a criminal complaint alleging violations of Title 18, United States Code, Sections 1028(a)(7) and 1029(a)(3).

6. This affidavit is intended to show only that there is sufficient probable cause for the requested criminal complaint and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Background concerning 'Darknet Markets'

7. A Darknet Market is a commercial website on the dark web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, other illicit goods as well as the sale of illegal products. Silk Road was the first popular Darknet Market (DNM) that operated from October 2011 until it was dismantled by federal law enforcement in October 2013. Following on from the model developed by Silk Road, contemporary markets such as Silk Road 2, Agora, and Alpha Bay are characterized by their use TOR, bitcoin payment with escrow services, and eBay-like vendor feedback systems.

Background Concerning Bitcoin

8. Based on my experience with cyber investigations, I know the following about Bitcoin: Bitcoin is a form of virtual currency, existing entirely on the Internet and not in any

physical form. The currency is automatically through computer software operating on a decentralized, "peer-to peer" network.

9. To acquire Bitcoin in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of conventional currency, which they exchange for a corresponding number of Bitcoin based on a fluctuating exchange rate.

10. When a user acquires Bitcoin, the Bitcoin are sent to the user's Bitcoin "address," analogous to a bank account number, which is designated by a complex string of letters and numbers. The user can then conduct transactions with other Bitcoin users, by transferring Bitcoin to their Bitcoin addresses, via the Internet.

11. No identifying information about the payer or payee is transmitted in a Bitcoin transaction. Only the Bitcoin addresses of the parties are needed for the transaction, which by themselves do not reflect any identifying information.

SPECIFIC PROBABLE CAUSE

12. On July 4, 2017, Janine and Steve Aversa, came home from vacation and noticed that two laptop computers and a women's gold necklace were missing from their residence, located at 1534 Holland Road, Holland, Bucks County Pennsylvania. Janine Aversa is the mother of Brittany Morton, and Steve Aversa is Brittany's stepfather. Aversa contacted Brittany Morton and questioned her, suspecting Brittany's boyfriend THEODORE PRICE as being responsible for the thefts. Aversa explained that PRICE is not allowed inside her home. Brittany Morton admitted to being at the Aversa home and to allowing PRICE into the residence.

13. On July 5, 2017, James and Brittany Morton came into the Northampton Township Police Department with two black laptop type bags. James Morton is Brittany

Morton's father. Detective Stark interviewed both. Brittany advised that her mother, Janine Aversa, notified her on July 4, 2017 of the two missing laptop computers. Brittany Morton then questioned THEODORE PRICE about taking the computers and he denied taking them.

14. Brittany advised that she drove PRICE on July 5, 2017 to Red Tree Tech, 303 W. Main Street Lansdale, PA for PRICE to have work done on his father's computer. Brittany advised that PRICE came out of the store and said that he sold the computer because it was not salvageable.

15. Brittany became suspicious of this and went back to the computer store after dropping PRICE off. She spoke with the store personnel, and located her step father's missing HP Pavilion laptop computer at the store. THEODORE PRICE had sold the computer to the store for $150.00.

16. Brittany further advised that she had rented a computer through Rent-a-Center a while back for PRICE to use. PRICE was responsible for making the rental payments on the computer. Brittany subsequently learned that PRICE had not been making the rental payments as he had promised.

17. Brittany traveled back to PRICE'S residence, which she also had access to, located at 2701 Elroy Road, Unit F4, Hatfield PA 19440, and removed two black laptop cases, believing that the cases contained the Rent-a-Center laptop she was responsible for and her mother's still missing laptop computer. She left the residence before being confronted by PRICE.

18. Brittany stated that she went through one of the computer bags and found PRICE'S wallet, which he had previously told her that he lost. Inside the wallet was a credit card bearing Brittany's father's name (James Morton). Brittany then contacted her father and relayed this information to him. (James Morton previously had filed a police report regarding a personal

check being stolen from him and being cashed against THEODORE PRICE'S Bank account).

19. James Morton stated that his daughter Brittany met him and that he went through the computer bags, looking for more of his information/property. In doing so, James Morton located more of his credit cards that were removed from his office at home, as well as credit cards he had ordered as replacements for the missing credit cards. James Morton advised that he had never received these cards in the mail and suspects that they were removed from his mailbox. Morton further stated that he located other mail in his name as well as credit cards bearing the name of his deceased mother (Ruth Morton) as well as Brittany's ex boyfriend (Matthew Karrman), all of which were previously located in his home office.

20. James Morton advised that while looking for more of his information, he located folders containing personal identifying information of people across the country, as well as a bunch of alphanumerical codes he did not understand.

21. At that point, James Morton thought it best to bring this information to the police station. Detective Stark subsequently ran THEODORE PRICE'S name through LEADS Online, a pawnshop and second hand sales database and found that THEODORE PRICE sold a Women's 14kt white gold necklace for $35.00 on 7/5/2017 at Tolls Jewelers in Huntington Valley, PA. This necklace was positively identified as Janine Aversa's necklace. Detective Stark recovered this necklace and spoke to the owner of the shop, Leslie Toll. Toll advised that when he purchased this jewelry from Price, he issued Price a white copy/ receipt of the transaction.

22. Detective Stark was subsequently contacted by Brittany Morton who advised that PRICE had utilized the Warminster Cash Exchange in Warminster Township to sell computer parts in the past. Detective Stark contacted the Warminster Cash Exchange and found that

THEODORE PRICE had sold two laptop computers on 6/29 /2017, one of which was an MSI brand gaming computer. Detective Stark contacted Brittany Morton who confirmed that the computer from Rent-a-Center was an MSI gaming computer, and provided the rental contract for the computer. Detective Stark went to the Cash Exchange, verified that the serial number on the MSI computer matched the serial number on the rental contract, and recovered the computer.

23. Detective Stark obtained a search warrant to search for and seize items from the two listed laptop computer bags. While searching this property, Detective Stark recovered numerous "Thumb" flash drives, two computers, multiple Micro SD memory cards as well as a piece of paper and a notebook which listed a victim' s name, address, phone number, credit card number to include a date of expiration as well as the three digit security code. Further investigation found a folder containing numerous pages of personal identification information to include people's names, addresses, social security numbers, and dates of birth, place employment, Internet Protocol addresses and phone numbers. There were also people's names with credit card account information. Additionally, Detective Stark located credit cards in the name of James Morton, Brittany Morton, Ruth Morton and Matthew Karrman within these bags. Detective Stark also located three pieces of mail in the two black bags which were addressed to "THEODORE PRICE, 2701 Elroy Road, Apt. / Unit F4, Hatfield PA 19440-4300."

24. Detective Stark also located a silver and black Hewlett Packard laptop computer and charging cord. Janine Aversa subsequently identified the computer as her computer. In turning on the computer to verify it was hers however, Aversa noticed that there are now programs on the computer that are not hers. Some of the new icons on the computer include the following names or information: "Tor Browser", "CyberGhost 6", and a folder called "Cain".

25. "Tor Browser" is a free browser that allows individuals to connect any internet

website through an anonymous IP address. Additionally, it allows users to connect to dark net only websites.

26. "CyberGhost6" is a free VPN offered for all operating systems. It can be used with Tor Browser, and has encryption abilities that CyberGhost6 claims are unbreakable. It contains a proxy web browser that fully encrypts all online traffic.

27. "Cain" is a reference to "Cain & Able", one of the most popular tools used for password recovery. It can recover various types of passwords using methods such as "brute force attacks, crypt analysis attacks, and . . . the dictionary attack." It is one of the most popular free hacking tools found on the internet.

28. Additionally, a folder containing approximately 105 pages of alphanumeric code was located during the search. Detective Stark contacted the U.S. Department of Homeland Security Special Agent Albert Cabrelli regarding these codes. He advised that he believed these codes to be "Bitcoin Wallets," which would potentially contain "Bitcoins," a type of internet currency used to purchase items on the "Dark Web." Cabrelli advised that the "Dark Web" is a type of alternative internet where illicit items ranging from personal identities, credit card information and narcotics can be purchased using these "Bitcoins."

29. On July 12, 2017, during the execution of a state search warrant at THEODORE PRICE's residence, SA Cabrelli identified himself to THEODORE PRICE and asked if he had any computer knowledge. PRICE stated that he had some. SA Cabrelli asked PRICE if he used "Tor" and, if so, what sites did he visit? PRICE stated that he visited AlphaBay.

30. SA Cabrelli asked PRICE how much Bitcoin does he own, at which time Price responded "not much if any." When asked by SA Cabrelli how he purchased merchandise on Alpha Bay, Price stated that he transferred money through "Paxful." SA Cabrelli knows

"Paxful" to be a peer-to-peer trading platform for bitcoin. When SA Cabrelli asked how he added money to his "Paxful" account, PRICE stated that he purchased Amazon Gift Cards at local conveniences and sold them through "Paxful." Once his account had a positive balance he would buy bitcoin to make his purchases on Alpha Bay.

31. SA Cabrelli asked PRICE what he purchased on Alpha Bay and how often he made purchases on the dark net. PRICE stated that he didn't make purchases that often, occasionally once or twice a month, but when he did make purchases it related to computer literature, specifically Remote Access Trojan (RAT) software.

32. Moments after the aforementioned statements, PRICE stated to SA Cabrelli that he lied about is computer knowledge, stating that his computer knowledge was rather extensive. When asked how extensive, PRICE stated that people hire him to do things for their companies. PRICE elaborated stating that he would write Trojan software to penetrate network systems. When asked what companies contracted him, PRICE stated to SA Cabrelli that he has been hired by numerous foreign governments to develop penetration software.

33. Subsequent to the search and seizure at the said residence in Hatfield, Price was later interview at the Hatfield Police Department by SA Cabrelli and Detective Stark.

34. SA Cabrelli and Detective Stark questioned PRICE about the number of bitcoin wallets found on the computer that PRICE accessed and was previously referred to James Morton as "bunch of alphanumerical codes."

35. PRICE stated that he purchased incomplete software from a vendor on Alpha Bay for approximately $50 USD. PRICE stated that he completed the software and executed a mass vanity address creator to simulate the same coding that blockchain uses to make Bitcoin wallets. PRICE stated for each Bitcoin transaction, there is a private key allowing you to access the

wallet. After recoding the program that he purchased on Alpha Bay, PRICE stated that he distributed his software using "Pastebin" injecting it to email addresses on specific internet forums.

36. SA Cabrelli knows "Pastebin" to be popular website for storing and sharing text. Though it is mostly used for distributing legitimate data, it is frequently used as a public repository of stolen information, such as network configuration details and authentication records. Various hacker groups and individuals also use Pastebin to distribute their software/malware.

37. PRICE stated that one of the Bitcoin wallet addresses that he possesses currently has a balance of over $34.6 million. PRICE stated that intended to use the collected bitcoin addresses to tumble the money back to another account where he would liquidate at another time. "Tumbling" refers to a method of concealing a bitcoin transaction trail by using a "tumbler" service to mix all transactions with others thereby breaking the connection between the address from which Bitcoin is sent and the address where it is received. This practice is also referred to as Bitcoin laundering.

38. PRICE stated that his software copies his bitcoin wallet to send or receive payment. PRICE'S software recognizes the similar characters in another wallet and replaces it with Price's acquired wallet. Because the bitcoin wallet address is a legitimate address, the user does not realize that bitcoin transaction is being diverted into a wallet other than theirs.

39. SA Cabrelli showed PRICE a printed 100 page document of Bitcoin wallets recovered during this investigation via search and seizure warrants. PRICE acknowledged the document and confirmed the $34.6 million bitcoin wallet exists within. PRICE continued that there are other Bitcoin wallets with thousands, some millions, of dollars.

40. PRICE stated that he would need either his computer or a computer that he could download his software to recover the money. PRICE stated that it would take too long to attempt to identify the wallet manually.

41. PRICE was asked to give access to his "Paxful" account, user name "Fulleffectreggie." PRICE cooperated and opened his account for SA Cabrelli and Detective Stark. SA Cabrelli noticed numerous transactions in the account activity utilizing bitcoin.

42. PRICE stated to SA Cabrelli that he had contacted a private jet service to leave the United Stated because he knew the police were coming for him. When asked where he was going to go, PRICE said the jet service would take him to a private airstrip in London.

43. PRICE stated to SA Cabrelli that he possesses a passport with the name "Jeremy Renner" and planned on assuming that identity to leave the country. When asked why he chose that name, PRICE stated that he like the movie the "Adventures" and Renner was an actor in the movie.

44. SA Cabrelli knows that Alpha Bay is a place on the Dark net where fraudulent information can be purchased, to include passports, stolen credit cards, and personal information of victims of fraud and/or deceased individuals.

45. PRICE stated that he purchased credit card "dumps" on Alpha Bay, explaining that the "dumps" consist of stolen credit cards and user information available for sale. PRICE stated that not every fraudulent credit card obtained works, claiming you don't know until you use it.

46. Detective Stark attempted to contact numerous people who had their personal information and/or credit card information located in the black computer bags. Detective Stark reached one individual who confirmed that the personal identifying information that PRICE had

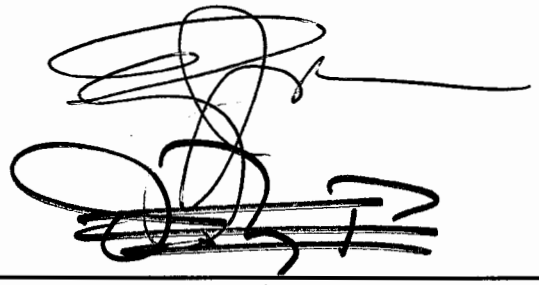
for her was correct. Likewise, Detective Stark reached 3 people whose credit card information was on the list and had been recently compromised, requiring them to obtain new credit cards.

47. The list possessed by PRICE and recovered from the black computer bags contained the credit card numbers and personal information of more than 15 people.

48. PRICE stated that he had been living in hotels in neighboring counties of Philadelphia purchasing the rooms through the website www.Expedia.com and using Bitcoin to pay for it. PRICE stated that he used his and fraudulently obtained Bitcoin to purchase the rooms.

CONCLUSION

49. Based on the foregoing, your affiant has probable cause to believe, and does believe, that PRICE has committed violations of 18 U.S.C. §§ 1028(a)(7) and 1029(a)(3): identity theft and access device fraud.



Special Agent Emily J. Evans
Homeland Security Investigations
Department of Homeland Security

Sworn and Subscribed to me
This 18 day of July, 2017.

HON. TIMOTHY R. RICE
U.S. MAGISTRATE COURT JUDGE